

FTC Remains on the Location Data Beat: Agency Settles Long-Running Kochava Enforcement, Even as State Regulation Has Already Changed the Landscape

New Media and Technology Law Blog on June 3, 2026

In early May, the Federal Trade Commission (“FTC”) [announced](#) a [proposed settlement](#) with digital marketing and analytics firm Kochava, Inc. (“Kochava”) and its subsidiary to resolve allegations the companies sold location data from hundreds of millions of mobile devices that could be used to trace individuals’ movements (*FTC v. Kochava Inc.*, No. 22-00377 (D. Idaho Proposed Stipulated Order May 4, 2026)). The proposed order, among other things, prohibits Kochava and its subsidiary from selling, sharing, or disclosing sensitive location data (absent a narrow exception) and requires them to implement a supplier assessment program.^[1]

The Kochava proposed settlement is the latest reminder that precise location data collected without adequate consumer consent remains an FTC enforcement priority, building on [similar agency settlements announced or finalized during the Biden administration](#)^[2] with data brokers and related providers (albeit with slightly narrower relief). Yet, given the agency’s enforcement history in this area and recent state-level privacy enactments, the settlement may be less a new frontier than a sign of where the market has already been pushed. The settlement reinforces the FTC’s stance that data brokers and their customers must confirm consent and screen for sensitive location data, as well as verify that data suppliers have obtained informed consent before collecting and sharing such data. At the same time, given the spate of state data privacy laws (including laws prohibiting the sale of precise location data), at least some industry participants may have already adopted sensitive location and related controls.

Brief Recap: Complaint and Enforcement

As we described in an earlier post, in August 2022 the FTC filed its original [complaint](#) (later a [second amended complaint](#)) against Kochava, seeking to halt Kochava’s alleged acquisition and downstream sale of “massive amounts” of precise geolocation data collected from consumers’ mobile devices “without consumers’ knowledge or consent,” in a format “easily linkable to individual consumers” that would allow third parties to track consumers’ movements to sensitive locations. The FTC alleged that Kochava, as a data broker, collects information about consumers tied to their mobile devices, uses records of precise geolocation over time to categorize consumers into audience segments, and sells those lists to others.

In May 2023, an Idaho district court [granted](#) Kochava’s motion to dismiss, with leave to amend. As we detailed in a prior post, [the FTC filed an amended complaint and successfully moved to have it unsealed](#). In February 2024, the court [denied](#) Kochava’s motion to dismiss the amended complaint and the agency subsequently filed a [second amended complaint](#), adding its subsidiary, Collective Data Solutions, LLC, as a defendant.

Proposed Settlement Terms

The current FTC appears to be keeping its enforcement eye on data brokers’ handling of precise location data, unsurprising given Chairman Andrew Ferguson’s prior statements as an FTC commissioner.[\[3\]](#)

Even after years of litigation, the proposed settlement ended up largely in line with the location data settlements the FTC reached in the past, with perhaps some narrowed relief. For example, the current settlement’s definition of “sensitive locations,” while relatively broad, uses more general terms or omits certain establishments from the Biden-era definition (e.g., labor union offices or locations predominantly serving LGBTQ+ individuals). Another difference is the Order’s 10-year term (versus 20-year terms in comparable Biden-era settlements). Despite these differences, the proposed settlement contains provisions that hew closely to prior FTC settlements, including:

- **Prohibition on sale or disclosure of sensitive location data:** An exception applies if defendants have a direct relationship with the consumer, the consumer has provided affirmative express consent and the data is used to provide a service directly requested by the consumer.

- **Sensitive location data program:** Defendants must develop a written program to develop a list of sensitive locations, updated quarterly, in order to prevent the sale or disclosure of such data. For sensitive location data where consent has not been confirmed, defendants must delete or render it non-sensitive within set time periods.
- **Supplier assessment program:** Defendants must maintain a program to ensure consumers have provided adequate consent to any supplier-provided location data (and cease using supplier-provided data for which consent has not been confirmed).
- **Consumer disclosures:** Defendants must provide *either* a clear means for consumers to request the identity of any recipient of their precise location data *or* a conspicuous method to request deletion from recipients' commercial databases.
- **Allow consumers to withdraw consent:** Provide consumers with a means to withdraw consent to use or disclose their device's precise location data and means to request that Kochava and its subsidiary delete precise location data previously collected.
- **Deidentify historical location data:** Deidentify or render non-sensitive all historical location data (absent data obtained with adequate consent) and send notices to customers that received historical location data within a set period.

Final Considerations

Given the FTC's track record in the location data privacy area, the Kochava settlement is not groundbreaking, particularly for data providers that already treat precise location data differently than ordinary browser tracking data and follow sensitive data best practices. The almost four-year period between the filing of this action and its resolution has shown the speed of developments in technology law and data privacy.

It seems that this enforcement has been eclipsed by subsequent legal developments since the FTC's past efforts in this area laid the groundwork for many principles in the proposed Kochava order. Since the original complaint, a growing number of states have passed data privacy laws based on either the California Consumer Privacy Act ("CCPA") or Virginia's more business-friendly privacy law (the "VCDPA"). Most comprehensive state privacy laws treat "sensitive data" (which can include precise location data) as a special category requiring heightened handling, though the specific language varies by state. Other states have passed more stringent requirements. For example, registered data brokers in California will soon implement the [Delete Request and Opt-out Platform](#) ("DROP"), a first-of-its-kind, state-created mechanism allowing Californians to send a single, verified deletion request to registered data brokers.^[4] Additionally, a handful of states have banned the sale of consumers' precise location data (with limited exceptions), with [Virginia expanding the VCDPA back in April 2026](#) and [Connecticut being the latest](#). Thus, by the time of the Kochava proposed settlement, many state privacy laws had already treated precise geolocation as sensitive data subject to heightened consent and use restrictions, with some states moving beyond consent toward outright sale restrictions.

Still, for data providers and their customers, this settlement reinforces the importance of diligence procedures surrounding location data products. With a Sensitive Location Data Program and other mandates required under the settlement terms, a customer's vendor due diligence efforts will likely examine more closely the sources, methods and maintenance of a vendor's program.

Overall, the settlement illustrates what robust operational compliance might look like: supplier assessments, ongoing sensitive location data reviews, consumer consent verification, data retention schedules and historical data remediation. It should be noted that long-standing location-data vendors may already have programs addressing these issues. For example, the Network Advertising Initiative (NAI) released [voluntary enhanced standards](#) for "Precise Location Information Solutions Providers" in 2022, updated in 2024, restricting the use, sale, and transfer of precise location information tied to sensitive points of interest.

However, customers conducting diligence may wonder if a vendor with an existing program can prove how close it is to the *Kochava* standards, from the quality of the sensitive locations list to downstream contract enforcement and the ability to trace whether a data feed contains sensitive location inferences.

While the FTC orders may give data ecosystem participants additional concrete diligence items, the consumer data collection process often remains complex and opaque. We will watch whether the Kochava settlement, along with further FTC statements and enforcements (and state-level enforcement), brings additional transparency about best practices surrounding the collection and use of location data.

[1] In a companion private civil class action over the same alleged conduct, the parties settled the matter in November 2025, with Kochava agreeing to various injunctive relief – though the plaintiffs did not release claims for monetary damages. (See [Murphy v. Kochava, Inc.](#), No. 23-00058 (D. Idaho Final Order Nov. 14, 2025)). Under the terms of that Settlement, Kochava agreed to implement several business practice changes, including a “privacy block” that filters and prevents dissemination of location data associated with Sensitive Locations, restrictions limiting any SDK-collected data to use by the originating app developer and permanent deletion of legacy SDK data retained for Kochava’s own benefit, a consumer opt-out and blacklisting mechanism, a verification process requiring Kochava to obtain representative consent prompts from data suppliers, and restrictions on use of data for machine learning purposes.

[2] Back in March 2024, we [wrote](#) about the FTC’s settlements with three business ventures engaged in the collection, use and sharing of certain sensitive consumer information (two actions involved location data, the third involved browsing-related information). About a year later, and in the waning days of the Biden Administration, the FTC resolved two more actions against data brokers engaged in the collection, use and sharing of location and sensitive consumer data ([In re Gravy Analytics, Inc.](#), [In re Mobilewalla, Inc.](#)), plus an additional settlement with an automaker over collection of location and driver behavior data ([In re General Motors LLC](#)), as the agency further developed its stance that the sale of non-anonymized, precise location data without the consumer’s informed consent is an unfair practice under Section 5 of the FTC Act. Both the Gravy Analytics and Mobilewalla proposed orders focus on data products related to “Sensitive Locations” (i.e., various locations that the FTC considers to be of a personal nature). For example, the FTC claimed Mobilewalla sold consumers sensitive location information associated with unique persistent identifiers that revealed consumers’ visits to sensitive locations and also sold access or insights into audience segments. In the General Motors (“GM”) [enforcement](#), the FTC alleged that GM collected precise geolocation and other data from GM-branded vehicles and then used and sold that data to third parties without drivers’ affirmative consent, resulting in consumers experiencing unexpected increases in auto insurance premiums or loss of coverage, as well as certain privacy harms.

[3] For example, in the [concurring and dissenting statement of then-Commissioner Andrew N. Ferguson](#) pertaining to the Mobilewalla and Gravy Analytics settlements originally reached in 2024, he concurred with the main thrust of the enforcements (even if he objected to the breadth of certain aspects of the relief):

“The FTC Act prohibits the collection and subsequent sale of precise location data for which the consumer has not consented to the collection or sale. It further requires data brokers to take reasonable steps to ensure that consumers originally consented to the collection of the data that the data brokers subsequently use and sell. If a company aggregates and categorizes data that were collected without the consumer’s consent, and subsequently sells those categorizations, it violates Section 5.”

[4] Connecticut's [SB 4](#), signed by the governor on May 27, 2026, requires the establishment of a California-style DROP portal by July 1, 2028, with Connecticut-registered data broker access beginning on October 1, 2028.

Related Professionals

- **Wai L. Choy**

Partner